US007004385B1

(12) **United States Patent**
**Douglass**

(10) **Patent No.: US 7,004,385 B1**
(45) **Date of Patent: Feb. 28, 2006**

(54) **CURRENCY DISPENSING ATM WITH RFID CARD READER**

(75) Inventor: **Mark Douglass**, North Canton, OH (US)

(73) Assignee: **Diebold Self-Service Systems division of Diebold, Incorporated**, North Canton, OH (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 62 days.

(21) Appl. No.: **10/814,100**

(22) Filed: **Mar. 31, 2004**

**Related U.S. Application Data**

(60) Provisional application No. 60/459,791, filed on Apr. 1, 2003.

(51) **Int. Cl.**
***G06F 17/60*** (2006.01)
***G06F 17/00*** (2006.01)
***G06K 5/00*** (2006.01)

(52) **U.S. Cl.** ..... **235/379**; 235/375; 235/380; 705/43

(58) **Field of Classification Search** ..... 235/375, 235/379–381; 705/35, 39, 43, 16, 17, 41, 705/44; 902/4, 5, 8, 12–14
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 6,338,048 | B1 * | 1/2002 | Mori | 705/41 |
| 6,578,760 | B1 * | 6/2003 | Otto | 235/379 |
| 6,601,771 | B1 * | 8/2003 | Charrin | 235/492 |
| 6,685,089 | B1 * | 2/2004 | Terranova et al. | 235/381 |
| 6,766,949 | B1 * | 7/2004 | Terranova et al. | 235/384 |
| 6,824,049 | B1 * | 11/2004 | Lee et al. | 235/380 |
| 2003/0057271 | A1 * | 3/2003 | Andersen et al. | 235/379 |

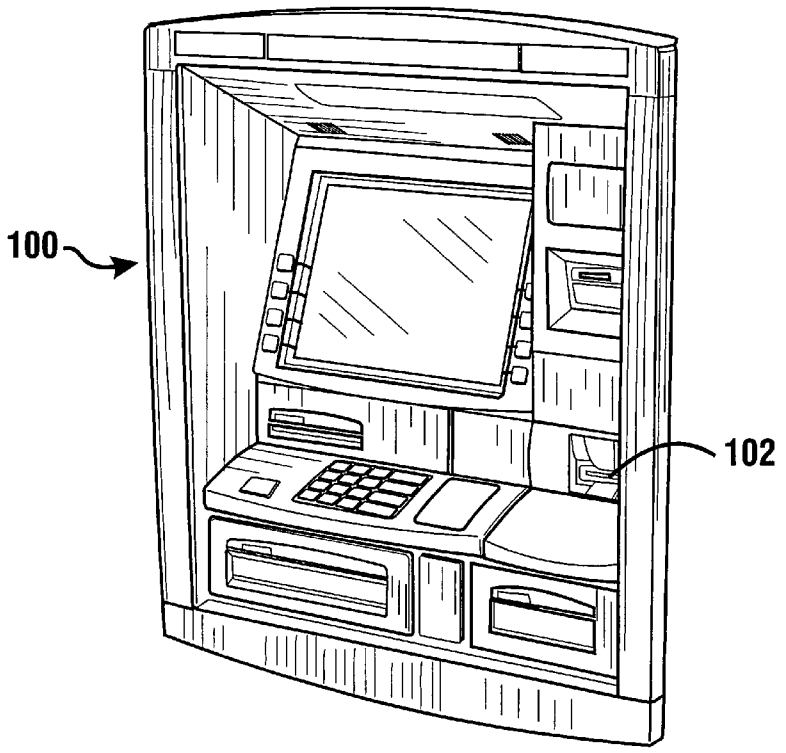
* cited by examiner

*Primary Examiner*—Karl D. Frech
*Assistant Examiner*—April Taylor
(74) *Attorney, Agent, or Firm*—Daniel D. Wasil; Ralph E. Jocke; Walker & Jocke

(57) **ABSTRACT**

An ATM with a currency dispenser includes a contactless card reader. The card reader can read data from an RFID tag of a customer's ATM card. An ATM RFID card reader can be located so as to provide additional space for another transaction component or can be used in conjunction with a magnetic stripe or other reader. Currency dispensing is enabled responsive to tag data. A housing is adapted to prevent interception of radio signals. The ATM is able to prevent dispensing of currency in situations where unauthorized detection of signals is sensed.

**57 Claims, 9 Drawing Sheets**



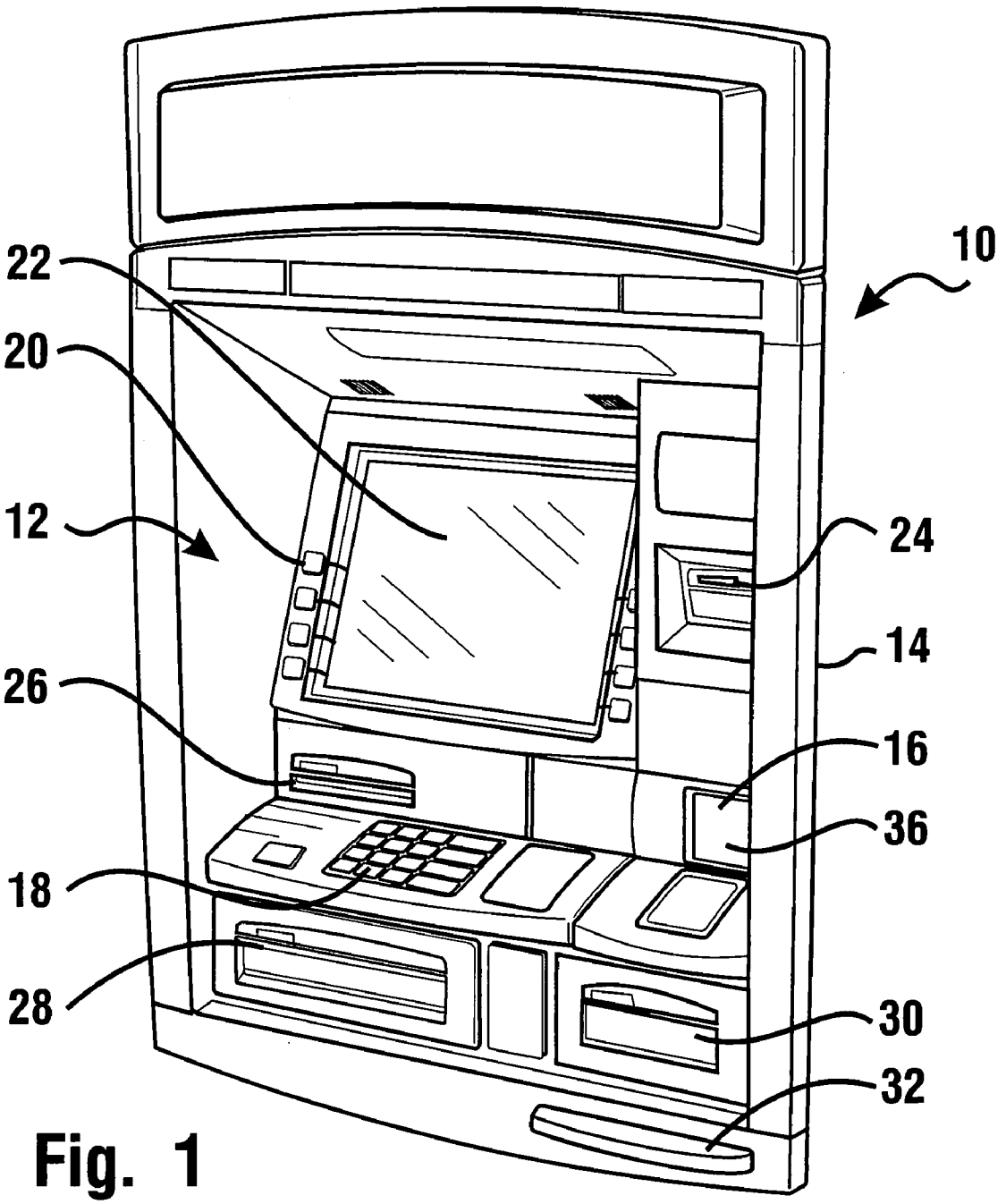



Fig. 1

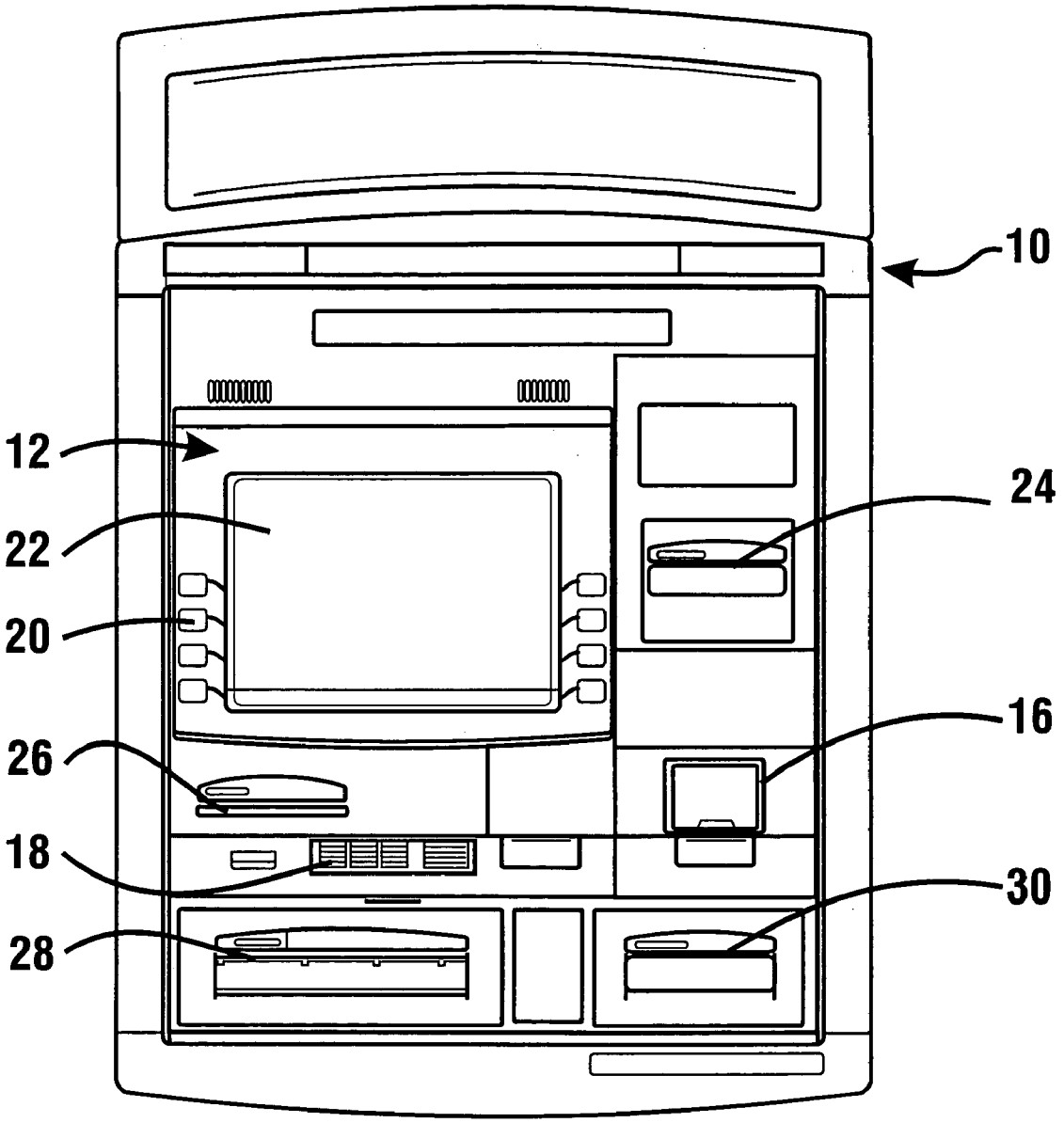



Fig. 2

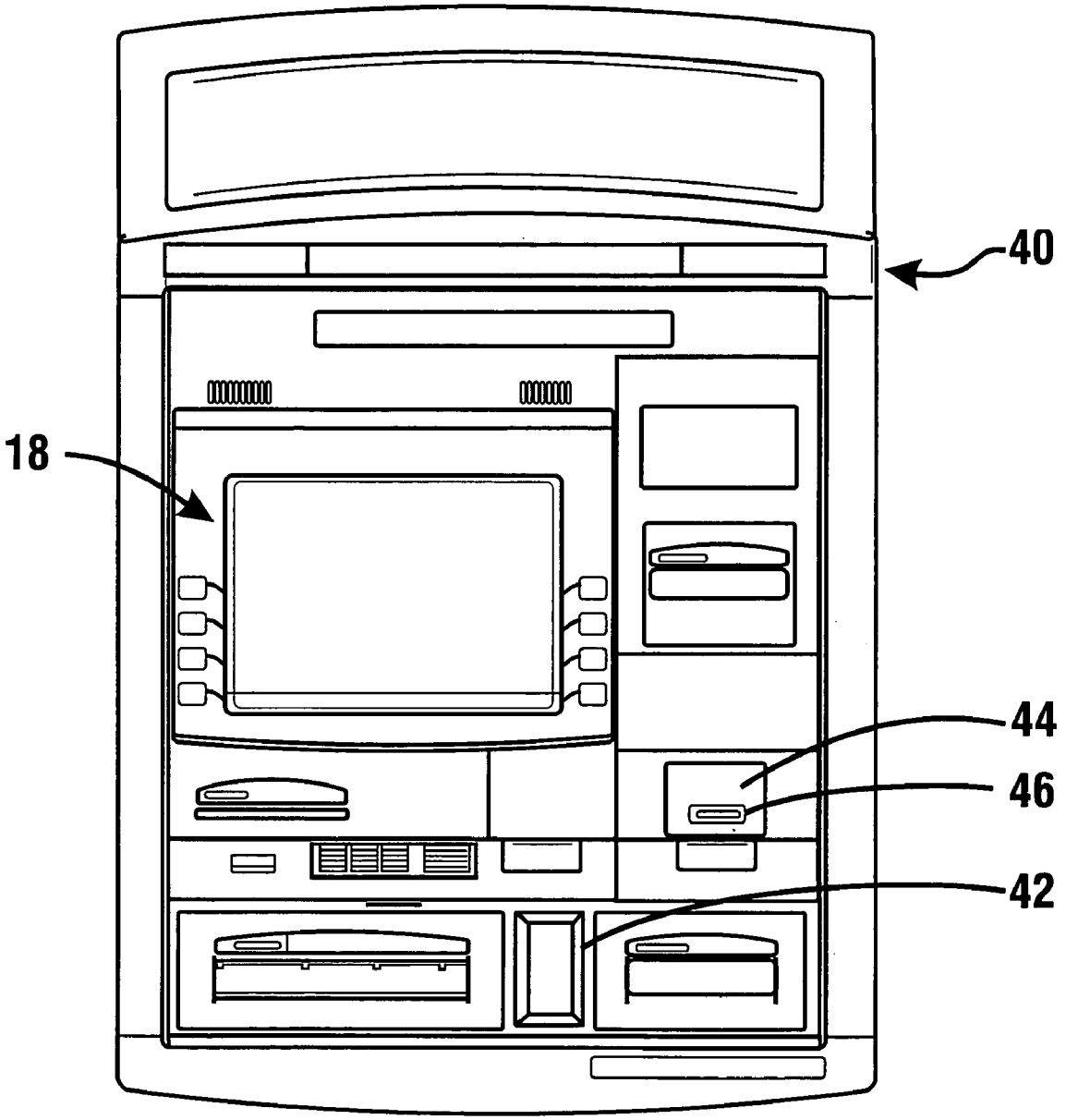



Fig. 3

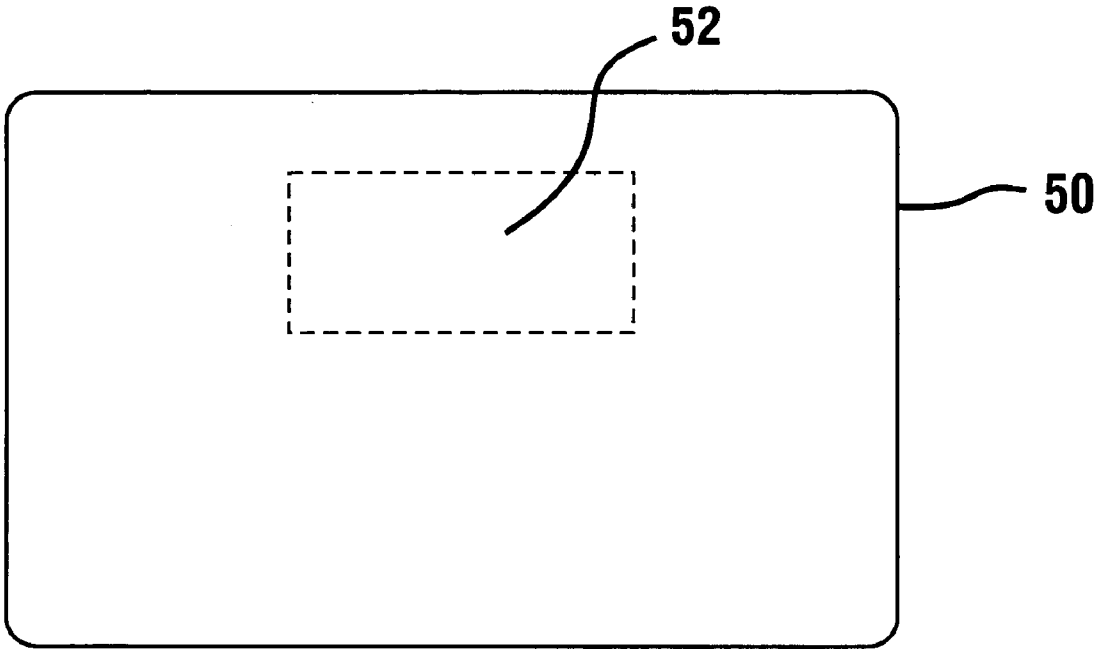



Fig. 4

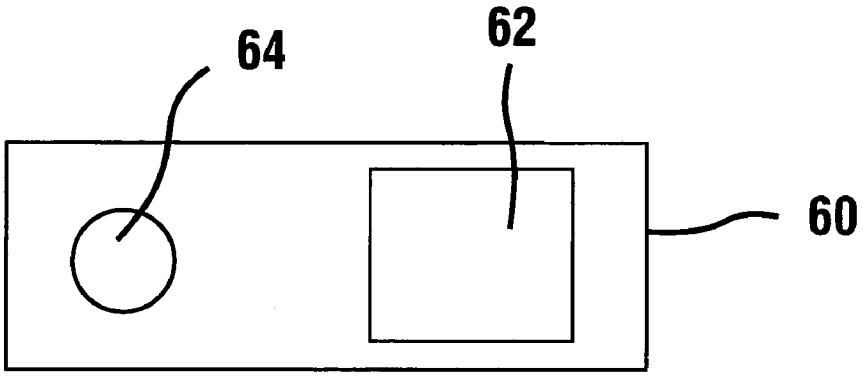



Fig. 5

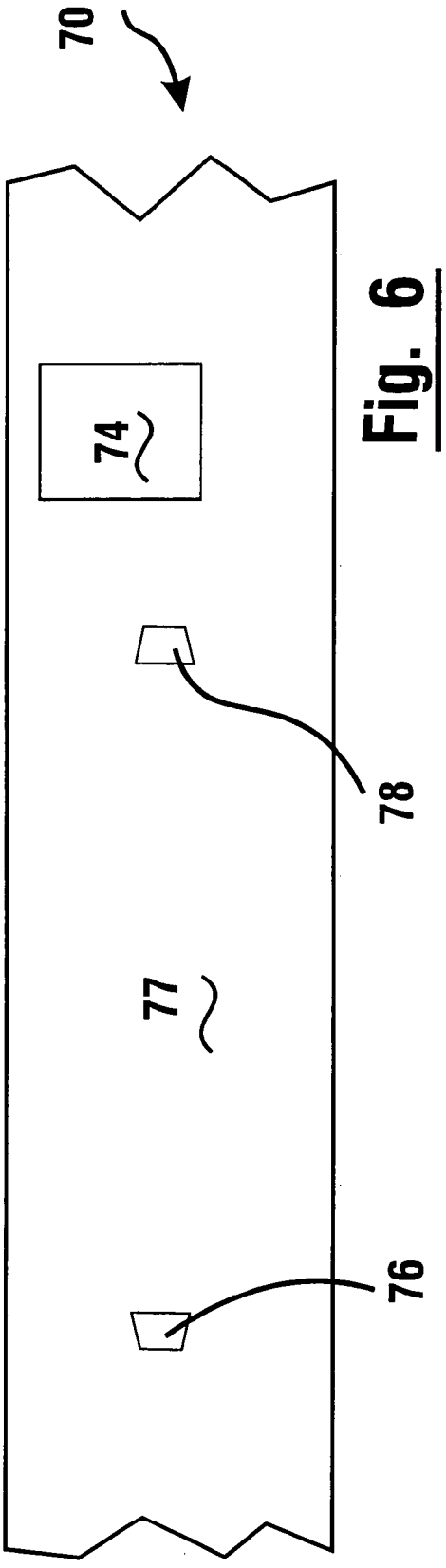



Fig. 6

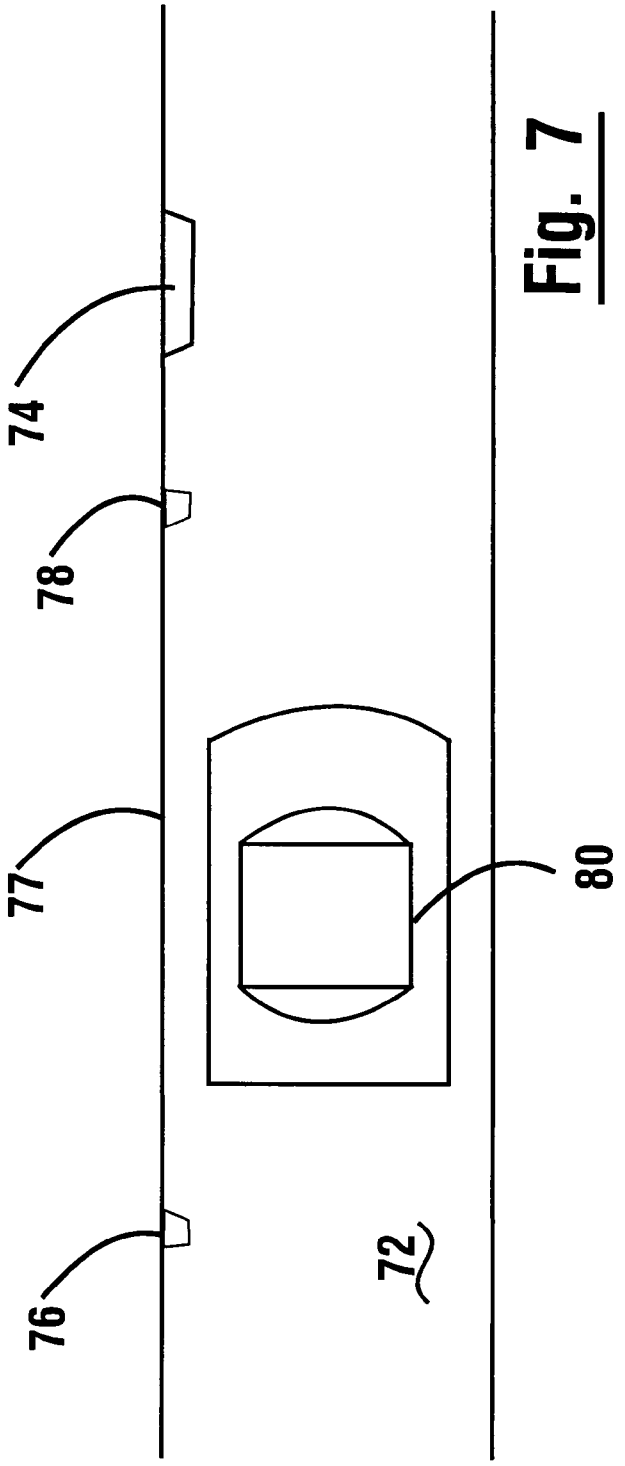



Fig. 7

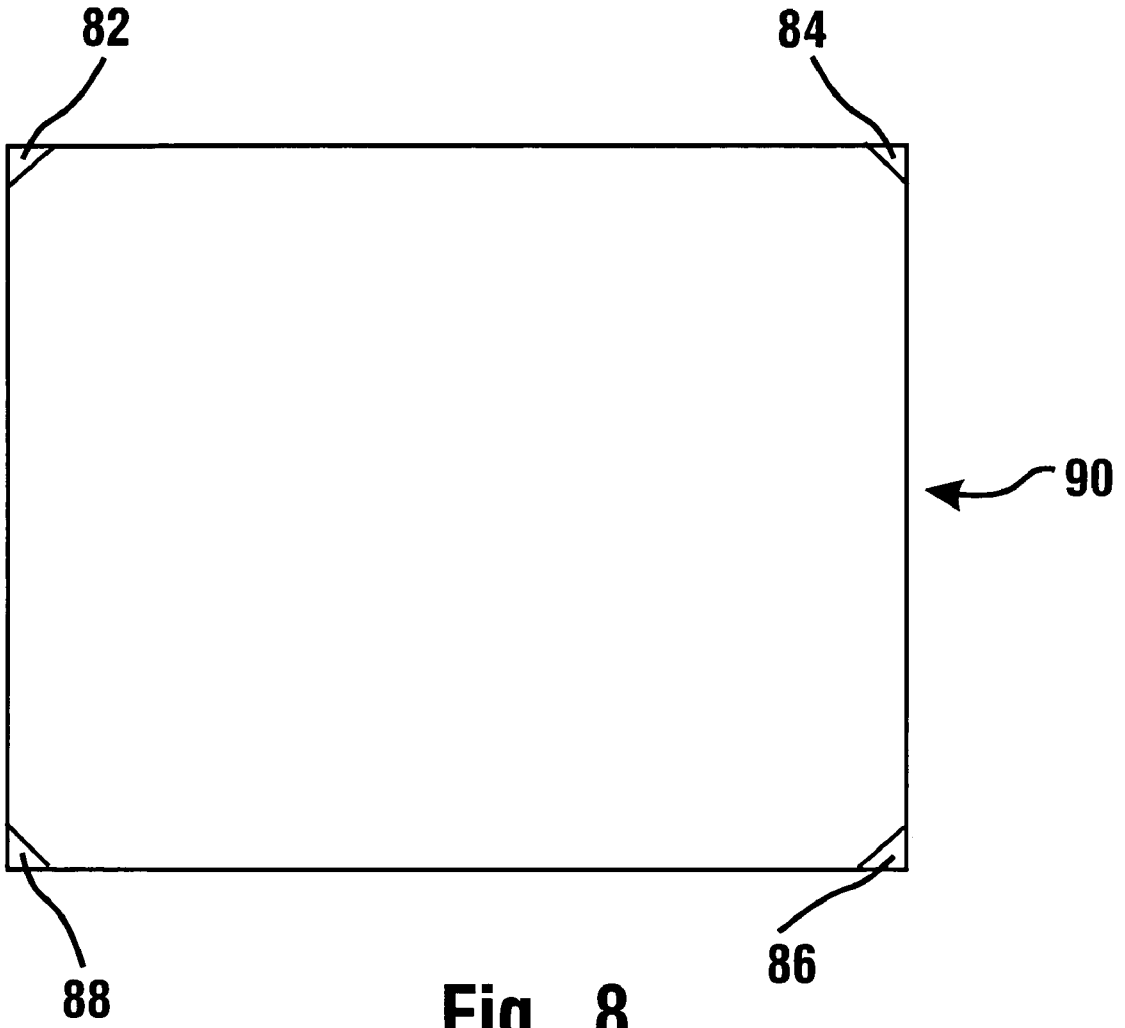



Fig. 8

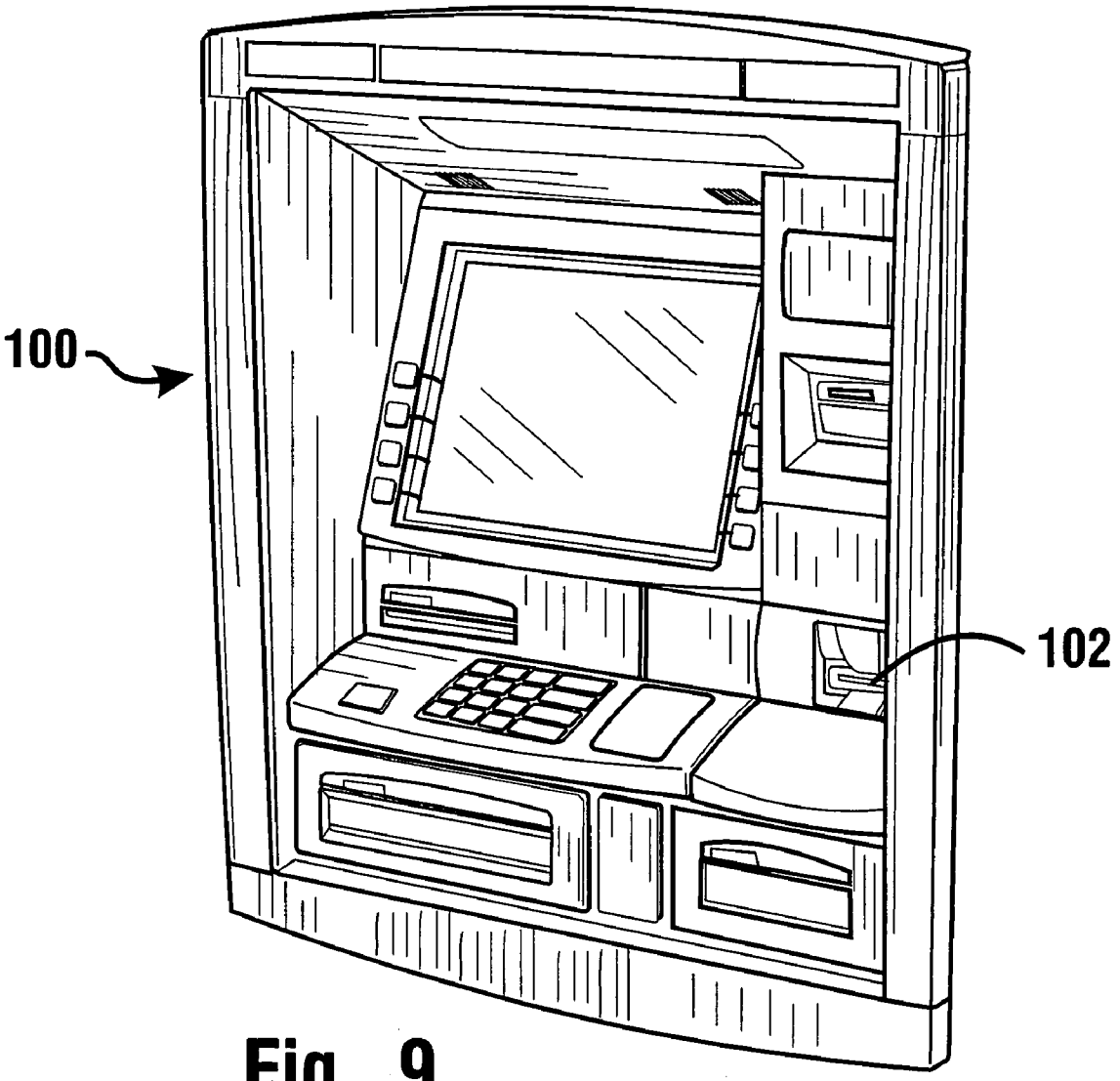



Fig. 9

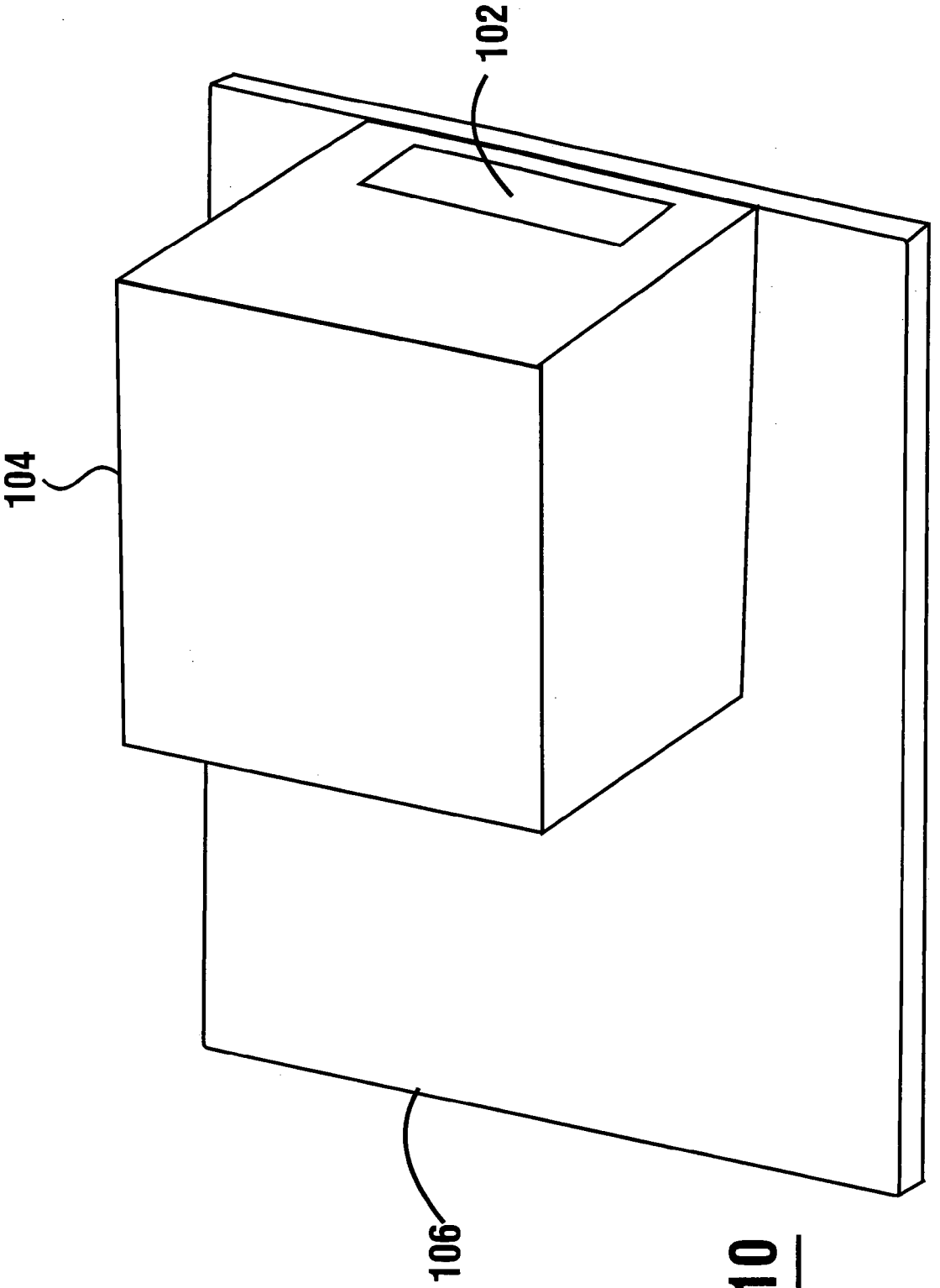



Fig. 10

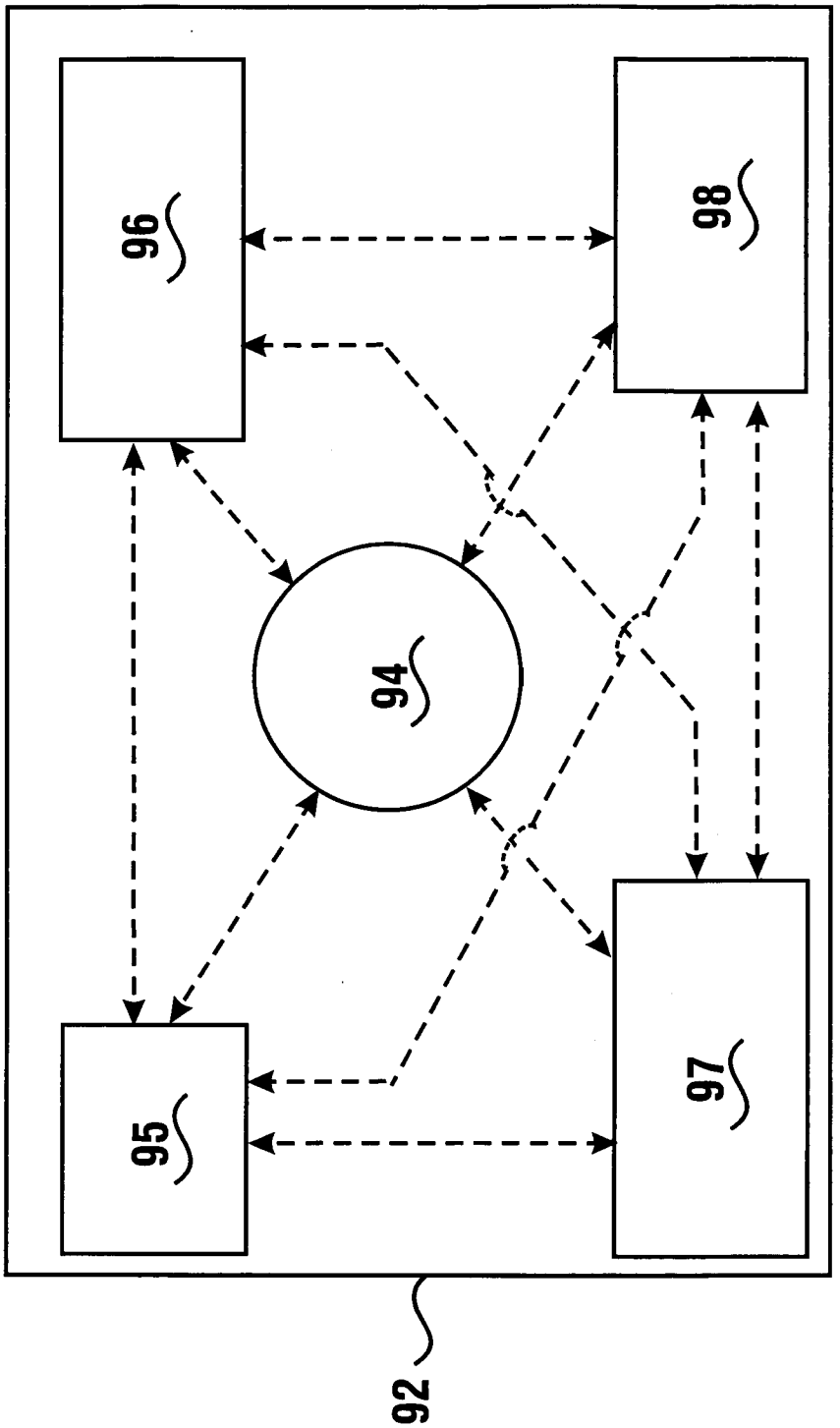



Fig. 11

# CURRENCY DISPENSING ATM WITH RFID CARD READER

## CROSS REFERENCE TO RELATED APPLICATION

This Application claims benefit pursuant to 35 U.S.C. § 119(e) of Provisional Application Ser. No. 60/459,791 filed Apr. 1, 2003, the disclosure of which is incorporated herein by reference.

## TECHNICAL FIELD

This invention relates to automated transaction machines. More specifically this invention relates to an automated banking machine apparatus and method that is capable of reading a user card in a contactless manner.

## BACKGROUND ART

Automated transaction machines include automated banking machines. A common type of automated banking machine is an automated teller machine ("ATM"). ATMs may be used to perform transactions such as dispensing cash, accepting deposits, making account balance inquiries, paying bills, and transferring funds between accounts. ATMs and other types of automated banking machines may be used to dispense media or documents such as currency, tickets, scrip, vouchers, checks, gaming materials, receipts, or other media. While many types of automated banking machines, including ATMs, are operated by consumers, other types of automated banking machines may be operated by service providers. Such automated banking machines may be used by service providers to provide cash or other types of sheets or documents when performing transactions. For purposes of this disclosure, an automated banking machine or ATM shall be construed as any machine that is capable of carrying out transactions which include transfers of value.

A popular brand of automated banking machine is manufactured by Diebold, Incorporated. Such automated banking machines are capable of receiving therein a banking card from a user of the machine. The card can have user information embedded in a magnetic stripe on the card. A machine card reader is capable of reading the magnetic stripe. The information may correspond to a user's personal identification number (PIN). The user generally can enter the PIN through use of a machine keypad. The machine operates either itself or in conjunction with one or more connected systems to determine whether the keypad-entered PIN matches the card-entered PIN. Upon determination of a match, the user can be authorized to carry out one or more transactions with the machine. Such a transaction may include dispensing cash such as currency notes to the machine user.

Magnetic stripe cards can have the problem of wearing out. Magnetic stripe cards are also susceptible to being duplicated. The contact head of a contact type card reader can be subject to excessive dirt accumulation or wear due to physical contact with cards. These conditions present the increased potential for fraud and/or requiring card reader maintenance which may place an automated banking machine out of service. The location and space required by a contact type card reader can also limit a machine from presenting additional banking features to a user.



## DISCLOSURE OF INVENTION

Thus, there exists a need for improvements to card readers used in automated banking machines. There further exists a need for card readers that can be readily installed in existing automated banking machines to increase the machine's functionality.

It is an object of an exemplary form of the present invention to provide an automated banking machine.

It is a further object of an exemplary form of the present invention to provide an automated banking machine with an improved card reader arrangement.

It is a further object of an exemplary form of the present invention to provide an automated banking machine with a card reader that requires less service.

It is a further object of an exemplary form of the present invention to provide an automated banking machine with a card reader that requires less fascia space.

It is a further object of an exemplary form of the present invention to provide an automated banking machine with a contactless card reader.

It is a further object of an exemplary form of the present invention to provide a method of reading a bank card with an automated banking machine.

It is a further object of an exemplary form of the present invention to provide a method for upgrading an existing machine to provide for improved card reading.

Further objects of exemplary forms of the present invention will be made apparent in the following Best Mode For Carrying Out Invention and the appended claims.

The foregoing objects are accomplished in an exemplary embodiment of the present invention by providing an automated banking machine with a contactless card reader. An RFID card and RFID card reader arrangement can be used instead of or as an adjunct to a conventional card and contact type card reader arrangement. A contactless card reader may be installed in new automated banking machines or in existing machines without further substantial modifications to the machines. Security risks may be reduced. As service issues could be reduced without the wear due to card reader head/card contact, use of a contactless card reader enables enhanced machine reliability at a modest cost.

## BRIEF DESCRIPTION OF DRAWINGS

FIG. **1** is a side schematic view of an automated banking machine.

FIG. **2** shows a front view of the automated banking machine of FIG. **1**.

FIG. **3** shows an alternative fascia of an automated banking machine.

FIG. **4** shows a card including an RFID tag.

FIG. **5** shows an alternative RFID card.

FIG. **6** shows a side view of an ATM drive-thru arrangement.

FIG. **7** shows a top view of an ATM drive-thru arrangement.

FIG. **8** shows a facility having plural RFID tag reading devices.

FIG. **9** shows an automated banking machine having a dual use card reader slot.

FIG. **10** shows an RFID reader is positioned adjacent to a magnetic stripe reader.

FIG. **11** shows an interior portion of an automated banking machine with components arranged in wireless communication.

IPR2025-01149
Apple EX1039 Page 11

## BEST MODES FOR CARRYING OUT INVENTION

Referring now to the drawings and particularly to FIG. **1** there is shown therein an automated banking machine, generally indicated by numeral **10**, used in connection with exemplary embodiments of the present invention. The automated banking machine **10** can be an automated teller machine (ATM). The automated banking machine **10** includes a fascia **12** which serves as a user or customer interface.

The automated banking machine **10** includes a housing **14** which houses certain components of the machine. The components of the machine can include input and output devices. The input devices may include a card reader schematically indicated **16**. Card reader **16** is operative to read a customer's card. The card can include information about the customer thereon, such as the customer's name, account number, and/or other data.

The fascia can include a keypad **18**, function keys **20**, display **22**, receipt outlet slot **24**, mini account statement outlet **26**, document (e.g., cash) withdrawal opening **28**, document deposit opening **30**, and a writing shelf **32**. It should be understood that these transaction function devices and features of the described ATM user interface are exemplary and in other embodiments the user interface may include different components and/or features and/or arrangements.

FIG. **2** shows a front view of the automated banking machine **10** of FIG. **1**.

The keypad **18** can include a plurality of input keys which may be actuated by a customer to provide manual inputs to the machine. The function keys **20** can be used to permit a customer to respond to screen prompts. The display **22** may be a touch screen display which enables outputs through displays on the screen and enables customers to provide inputs by placing a finger adjacent to areas of the screen.

It should be understood that in various forms of the invention other types of input devices may be used, such as biometric readers that may be operative to receive customer identifying inputs such as fingerprints, iris scans, retina scans, and face topography data that provide data that is usable to identify a user. Other input devices such as speech or voice recognition devices, inductance type readers, IR type readers, and other types of devices which are capable of receiving information that identifies a customer and/or their account may also be used. An example of an ATM that uses biometric input devices and other types of input devices is shown in U.S. Pat. No. 6,023,688 the disclosure of which has been fully incorporated herein by reference.

The output devices of the automated banking machine **10** may include the display **22**. The display can enable outputs through a display screen. The display **22** may include an LCD, CRT or other display type that is capable of providing visible indicia to a customer. The display **22** may be a combined input and output device, such as a touch screen display, which is capable of providing outputs to a user as well as receiving inputs.

The automated banking machine **10** may also include a receipt printer that is operative to print receipts for users reflecting transactions conducted at the machine. Exemplary embodiments may also include other types of printing mechanisms such as statement printer mechanisms, ticket printing mechanisms, check printing mechanisms, and other devices that operate to apply indicia to media in the course of performing transactions carried out with the machine.

In other embodiments output devices may include devices such as audio speakers, IR transmitters, or other types of devices that are capable of providing outputs which may be perceived by a user either directly or through use of a computing device, article, or machine. Exemplary automated banking machine features and systems are further shown in U.S. Pat. Nos. 6,705,517; 6,682,068; 6,672,505; and 6,598,023, the disclosures of which are incorporated herein by reference.

In an exemplary embodiment discussed in more detail herein, an automated banking machine may use contactless reading devices or arrangements or techniques to obtain information from or about a customer. A non-contacting card reading device may be used. Unlike conventional contact type card reading which involves physical contact, the exemplary embodiments permit card reading to occur without requiring physical contact.

For example, a customer bank card may include an indicator member such as a non-contact transponder to communicate with the automated banking machine. Radio frequency (e.g., radio waves) can be one manner in which to communicate in a non-contact relationship, e.g., communication not based on physical contact. Radio frequency (RF) type readers and/or RF transmitters may be used. Other types of remote communication may also be used.

A customer bank card may have one or more radio frequency identification (RFID) tags (or devices or indicator members). RFID tags may also be referred to as "smart labels." The tags can contain data indicative or reflective of customer information. RFID tags may operate on the RF backscatter principle. Data communication can occur between an RFID tag and a card reader **16** of an automated banking machine. An RFID reader may be able to interrogate the RFID tag to obtain information therefrom. RFID readers may also be referred to as "interrogators." In exemplary embodiments, an RFID tag may be of a type that does not need a power source (e.g., battery), but operates based on RF energy provided by a reader. A tag may also have an internal antenna embedded in an RFID chip. An RFID reader can be equipped with the power necessary to activate the chip and receive the stored information therefrom. The RFID tags and readers discussed herein may have RFID Industry Standards developed by ANSI (American National Standards Institute) or the International Standards Organization (ISO) or other standard developing organizations. For purposes of this disclosure an RFID tag will be considered to include any device which provides data output via RF signals, whether separate from or integral with another article, such as for example, a card.

A customer bank card may include information in non-contact RFID tags instead of or in addition to information in magnetic stripes and/or information in a programmable memory of a smart card. That is, magnetic stripe (or magnetic strip) cards and smart cards may further include customer RFID tags. One or more tags may be removably attached or mounted to a card (e.g., thereon or therein). Alternatively, tags may be permanently affixed to a card, such as embedded in a (plastic) portion of a card.

In an exemplary embodiment an RFID tag is operative to store information therein representative of or corresponding to a customer, such as the customer's account number, PIN, name, primary bank, affiliated banks, and/or preferences. In an exemplary embodiment, tags can contain much more customer-related data than can be represented by a magnetic stripe (or magnetic strip) type of arrangement. For example, tags may also contain information reflective of additional security features, customer profile data, card age, display

IPR2025-01149
Apple EX1039 Page 12

preferences, etc. A tag may also carry a unique customer identification number of 32 bits or longer. The tags can enable a card to store more information in a smaller space in comparison to prior art magnetic stripe cards.

RFID tags do not require physical contact (e.g., mechanical or electrical contact) with a card reader component. In an exemplary embodiment a customer can pass or wave their card adjacent to or over a card scanning area **36** associated with the card reader device **16** to have the card data (and user information) remotely read. The scanning area **36** can comprise a surface area of the ATM fascia. A card reader and an RFID card can be remotely separated during reading of the card. RFID cards may be more difficult to counterfeit. The contactless arrangement can prevent damage or deterioration (such as dirt accumulation, wear and tear) to a card reader, and may further reduce machine down time associated with maintenance and service.

RFID tags may have read-only or rewritable memory for storage of customer information. RFID tags may have a memory which can be changed or modified by authorized personnel or devices. The tag memory may be programmable. For example, an employee associated with a bank may have a device operative to communicate with an RFID tag to change and/or insert data contained therein. A handheld RFID tag communication device may also be used. Alternatively, an automated banking machine may incorporate a device for changing RFID data.

Alternatively, a tag may have unchangeable data. In such alternative situations, a combination of plural read-only tags may need to be assigned or attached to a particular card to fully represent its information content. A card may also have a combination of read-only and programmable tags.

An RFID reader device of an exemplary automated banking machine can be equipped to remotely read a user card. The reader is operative to read card data while the card is not in physical contact relationship with the machine. Thus, a card can be spaced from the card reader device during card reading. For example, a card reader device can be arranged to read RFID card data as a customer passes their card adjacent to a card scanning area associated with the card reader device. It follows that communication between a bank card and an ATM card reader can occur without physical contact, which would occur with the use of conventional contact type (e.g., magnetic stripe) card readers.

Because the physical aspects of a through-the-fascia portion of a contact type card reader interface can be avoided, the service and/or reliability issues for an RFID card reader compared to other type readers can be reduced and/or eliminated. Also, the wear of components (e.g., contact read head, mechanical card transports, and card sensors) associated with conventional contact type card readers can be eliminated. Furthermore, wear to a user's card can also be reduced.

When a card having an RFID tag is within range of an ATM card reader, the reader device circuitry can interrogate the tag to receive information corresponding to the particular card/user. The reader circuitry may comprise a circuit card assembly. The information exchanged between a card RFID tag and a card reader may be encrypted to provide additional security. Thus, a card reader, RFID data from the card, and/or an associated device may comprise a decoder in decoding circuitry.

The use of RFID reader technology permits an ATM to have a card reader located at a previously unacceptable position. The physical space of an RFID card reader and any RFID card reader interface (e.g., card scanning area) can be located at an area of the fascia different from the area previously required for a contact type card reader. Also, in some embodiments all or a portion of the RFID card reader device can be remotely mounted adjacent to the ATM. That is, an RFID card reader device need not be mounted on the fascia or ATM, but may be disposed from the ATM. An RFID card reader device can be positioned so as to free up fascia space for additional transaction devices, thus increasing an ATM's functionality. The freed up space allows other devices to be added to the valuable customer access area. For example, the additional fascia space may be used for installation of a cash acceptor, a stamp dispenser, check acceptor and/or an event ticket printer. Alternatively, in some embodiments the ability to eliminate the conventional card reader on the fascia can be used to produce more compact machines and/or user interfaces.

FIG. **3** shows an automated banking machine **40** similar to the automated banking machine of FIG. **1**. However, the machine fascia **48** is shown with an RFID card reader **42**, stamp dispenser **44**, and a stamp dispenser outlet **46**. The ability to use an RFID card reader **42** permits a stamp dispenser to be included in the machine instead of a contact type card reader. That is, the space previously needed for a contact type card reader can now be used by an additional transaction device, such as a stamp dispenser.

FIG. **4** shows a card **50** having an RFID tag **52** embedded therein. The RFID card **50** may also contain conventional card markings and indicia (e.g., raised numbers/letters) thereon. The card may be similar to a conventional ATM banking card or other debit or credit card, except having an RFID tag instead of or in addition to a magnetic stripe.

FIG. **5** shows an RFID card **60** having an RFID tag **62** thereon and a key hole **64**. In an exemplary embodiment, a user card only needs to be of a size large enough to hold an RFID data tag (or tags). In comparison to conventional ATM cards, the size of an RFID ATM card can be reduced. For example, an RFID card (as shown in FIG. **5**) may be of a size enabling its attachment to a key chain.

A card may have more than one RFID tag. The tags may be of different sizes and include different information. A card may have one or more tags embedded therein and/or one or more tags thereon.

The exemplary RFID cards **50**, **60** are usable with the automated banking machines **10**, **40** having the RFID card reader devices **16**, **42**. In such use there may be no need for a customer to insert their RFID card into an ATM machine. Nor does the machine need a card entry slot. Because the user card is not inserted into the ATM, the card cannot be "lost" in a fascia opening (e.g., card entry slot) or the machine. User stress related to fear that their card will not be returned by the machine can be eliminated. Potential users previously reluctant to use an ATM because of such fear can use an ATM without the worry of their card being lost in or captured by the machine. Thus, an ATM using an RFID card/card reader arrangement can be more user friendly. Because an ATM card can remain with the user at all times, the arrangement can also reduce or eliminate fraudulent schemes to trap a card or skim card data. Thus, an ATM using an RFID card/card reader arrangement can also provide enhanced security.

The use of an RFID tag arrangement can permit quicker ATM response time. For example, an ATM can automatically read the tag information, process the information, and prompt the user by name to enter a PIN number. The time previously necessary for the user to correctly insert their card into the ATM and have the card transported to/from the (contact type) card reader can be eliminated. The use of an RFID tag and RFID tag reader arrangement can reduce the

IPR2025-01149
Apple EX1039 Page 13

average time a user spends at an ATM. Thus, an ATM equipped to read an RFID data tag can increase usage efficiency of the ATM.

In other exemplary arrangements an ATM card can have an RFID tag with a programmable memory. The tag memory is able to store data corresponding to one or more recent account transactions. The ATMs have a writer device for updating the card's tag memory with the latest transaction data (e.g., bank name, cash withdraw amount, and date). The writer may be part of a combined RFID tag reader/writer device. The transaction data can act as a transaction receipt or a series of receipts. The card owner may have a computer that can wirelessly read the RFID tag to obtain the transaction data from the card memory. The computer can have the transaction data automatically downloaded into a home financial computer program, such as Quicken. The financial program can apply the transaction data to update the user's account. The ATM writer device can supplement or overwrite the data stored in tag memory. If necessary, the card owner can erase the tag memory after reading the data through operation of their home computer. In other arrangements which are described in more detail hereinafter, the transaction data in the RFID tag can be automatically read from a distance. For example, a card memory may be read without its removal from a user's wallet or purse. A user may have a smart house in which the RFID memory data can be read by a reader and delivered to the user's PC for input to a financial computer program. The structure of a smart house may enable the card memory data to be read upon the card (with the owner) entering the house, and then load the transaction data into the financial program. In alternative embodiments this can be done with a reader attached to the PC and the user bringing the card adjacent the reader at an appropriate time during operation of the financial program.

An ATM RFID data tag may also be inserted onto (or combined with) a typically non-ATM card (e.g., merchant charge card, ID card, drivers license, library card, etc.). The hiding of ATM information in a typically non-ATM card can increase the level of user information security.

Other arrangements can have an ATM RFID data tag on a multi-use card having plural distinct RFID tags. For example, the same card may have several RFID tags, each only usable for a specific purpose. One tag can be an ATM tag which is readable by an ATM, whereas another tag is a fuel purchase tag readable by a fuel pump, whereas a further tag is a credit card tag. Also, a multi-use card may have a generic RFID data tag which is readable by a plurality of RFID reading devices. The generic RFID data tag can include information which can be used in conjunction with data provided by or stored in one or more other tags on the multi-use card.

In certain exemplary RFID card reader arrangements an RFID card can be remotely read without the need to wave or place the card adjacent to or in close proximity of the card reader. For example, an RFID card reader can have an increased (e.g., in power) reading range capable of reading an RFID card while the card is still in a wallet/purse.

In alternative arrangements the ATM RFID data tag need not be on/in a card, but may be associated with a non-card item. For example, an RFID tag may be associated with a wallet or purse. The tag could be embedded in the wallet. Other items such as eye glasses, keys, and clothing may also be used to hold an RFID tag. The tag may be positioned at any location associated with a customer that enables its reading thereof by an RFID tag reader associated with an automated banking machine.

A vehicle (e.g., an automobile) may also be equipped with an ATM RFID data tag. The RFID tag may be positioned on the auto at any location enabling its reading by an appropriately placed RFID reading device of the ATM. For example, an RFID reading device may be situated to read a tag positioned on a window, mirror (e.g., rear view mirror), or license plate of an auto. The ATM can automatically read the tag information as the auto is approaching the ATM fascia, process the information, and prompt the user by name to enter a PIN number. That is, the speed of one or more computers associated with an ATM may be able to present a welcome display screen to a particular named customer prior to (or simultaneously with) that customer actually arriving (or stopping or parking) at the ATM. The use of an ATM RFID data tag on an auto can enhance speed and efficiency of drive-thru ATM banking.

FIG. **6** shows a side view of an exemplary ATM drive-thru arrangement **70**. An ATM **74**, RFID reading devices **76**, **78**, and a wall **77** are also shown. FIG. **7** shows a top view of the arrangement of FIG. **6** with the addition of a vehicle **80** in a drive-thru lane **72**. The vehicle **80** is approaching the ATM **74**. The reading devices **76**, **78** are operative to respectively read an RFID tag located in a front or rear view of the vehicle. The reading device **76** is positioned to read a tag from the rear of the vehicle, whereas the reading device **78** is positioned to read a tag from the front of the vehicle. The reading devices are in connection (e.g., wire or wireless connection) with the ATM.

In other exemplary embodiments, an ATM is able to recognize and prioritize a plurality of customers in a queue via (automatic) reading of their ATM RFID tags. The ATM can create a temporary memory list of users currently awaiting access to the machine. The memory can be stored in a first in first out (FIFO) method. The RFID reader of the ATM can be equipped to automatically read all ATM RFID tags within a predetermined distance of the reader/ATM. For example, the reader may be arranged to obtain (and provide to an ATM processor) information on all users in a queue within ten feet of the ATM.

This information can be used to determine personalized presentations to be made to the particular user once they reach the ATM. This may be done in a manner like that shown in U.S. patent application Ser. No. 09/449,426 filed Nov. 24, 1999, the disclosure of which is incorporated herein. Alternatively or in addition, the reader may be arranged to obtain information on a predetermined number of users. For example, the ATM memory may only concurrently hold information on three users. An ATM may also periodically scan for potential users to update the user queue memory. An ATM can be programmed to provide a special display message (e.g., apology, discount information) or dispense a coupon to a user who has waited a predetermined amount of time. Other items or services, either through machine display or through machine dispensing, may also be provided to customers that had a lengthy wait. Such other items or services may further include credits, rebates, tickets, refinance discount, free car wash, currency, special offer, or other form of benefit.

An ATM may also have a user option of canceling a (wrong-named) user who has left the queue subsequent to the latest queue update. That is, if the welcome display screen (which can refer to a particular user name) presented to a user corresponds to the wrong user (e.g., a user who has left the queue without detection by the machine), then the user who currently has access to machine can notify the machine of the situation. For example, the display screen may have an initial user message welcoming a specific user

IPR2025-01149
Apple EX1039 Page 14

along with a smaller message such as "If you are not the named user then please press the exit button." If the exit button is activated, then the ATM is able to quickly change the welcome screen to the user next listed in the queue memory. In some embodiments the queue data may be rechecked by the ATM scanning for signals of cards in proximity to the machine. Thus if the RFID signal associated with a particular user is no longer sensed, that user may be eliminated from the queue in ATM memory.

The ability of an automated banking machine (e.g., ATM) to recognize and prioritize a plurality of customers can permit a facility to offer additional customer amenities. A prioritizing automated banking machine can be equipped with speakers and a speech program to enable the machine to announce the name of the next customer granted access to the machine. A customer waiting area may be provided with seats (e.g., chairs) or tables enabling customers to sit and relax (or perform work) while they temporarily wait. The waiting area may also have a wall mounted display screen that is viewable to the entire waiting area. The automated banking machine can display the name and/or picture of the next customer on the screen. Other methods of notifying the next machine user can also be used. For example, the machine (or the machine's network host) may notify the user via a page or phone call to a cell phone.

In other exemplary embodiments a prioritizing automated banking machine may be used in waiting facilities where many people are normally expected to simultaneously congregate and wait, such as doctors' offices, hair stylist centers, and motor vehicle registration centers (e.g., DMV, BMV). A prioritizing machine may also be provided in a restaurant, such as a fast-food facility. The prioritizing device(s) can be operatively connected to one or more remote tag readers to automatically read all RFID tags in a predetermined area of the waiting facility. For example, the tag readers may be strategically positioned to generally surround the waiting area. FIG. **8** shows a waiting facility **90** having RFID tag reading devices **82**, **84**, **86**, **88** positioned in a surrounding relationship. The reading devices are operatively connected to a prioritizing device. The reading devices may be sequentially or simultaneously operated.

In an exemplary embodiment, contactless (e.g., wireless) technology can also be used by an automated banking machine to communicate not only with RFID tagged items (e.g., ATM cards), but also with other user devices, such as smart cards, PDAs (personal data assistant), cell phones, pagers, and laptop computers that utilize RF and/or RFID technology to send/receive data.

It should be understood that exemplary embodiments of automated banking machines may include a magnetic stripe reader in addition to RFID readers and/or writers. For example, an automated banking machine can have both an RFID tag reader and a magnetic stripe reader. The RFID tag reader can be combined with or positioned adjacent to the magnetic stripe reader. Such an arrangement enables two different types of cards to be read at generally the same location. The ability of an automated banking machine to read data from different types of data cards can be beneficial to implement the capabilities of reading more types of cards or during a transitional period of switching from magnetic stripe cards to all RFID cards.

An ATM can have a user card input slot (or card reader inlet) for insertion therein of an ATM card by a user of the ATM. The card insertion slot is able to receive both magnetic stripe cards and RFID cards. That is, the slot can be a dual use input opening. The slot can be aligned with a magnetic stripe reading device. The magnetic stripe reader can communicate with the slot via a pathway. The magnetic stripe reading device can include a housing that is able to receive the card therein. The slot can be a fascia opening and/or an entry into the magnetic stripe reader housing. The RFID tag reader can be positioned adjacent to the magnetic stripe reader, either in or out of the housing. In an exemplary arrangement the RFID reader is positioned outside of the housing. The housing can be of a structure (e.g., open or slotted) and/or of a material (e.g., plastic) that enables the RFID tag to be read exterior of the housing. FIG. **9** shows an automated banking machine **100** having a user card insertion slot **102** into which both magnetic stripe and RFID user cards can be inserted for reading by the machine. FIG. **10** shows cut away angled view of the card insertion slot **102** in relation to a magnetic stripe reader housing **104**. An RFID reader **106** is positioned adjacent to the magnetic stripe reader housing **104** in the automated banking machine **100**.

The card reading processes can be prioritized based on programming associated with one or more controllers in the automated banking machine. For example, the RFID tag reader can be controlled to operate first in attempting to read a card. Upon a successful read by the RFID reader, the magnetic stripe reader is not active. However, if the RFID reader's attempted read was unsuccessful, then the magnetic stripe reader is operated in a second attempt to read the card. If the second attempt is unsuccessful, then the card is returned to the user. In another reading program, the magnetic stripe reader can be operated first and the RFID reader second. In other card reading processes the magnetic stripe reader and the RFID reader can both be simultaneously operated to read a card.

In other exemplary embodiments the RFID reader may be positioned adjacent to the read head or other magnetic stripe reading device. In such embodiments the RFID tag and magnetic stripe data may be read generally simultaneously. Alternatively or in addition, the RFID reader may be read as data is read from a chip on a smart card. Of course, these approaches are exemplary.

In some embodiments it may be advantageous to read the RFID data from the card within the machine. In such machines it may be advisable to insulate the interior of the machine and/or the reader with RF signal blocking materials (for example conductive elastomers), such that RFID signals read from the card cannot be intercepted by unauthorized reading devices attached to or near the machine. Likewise such capabilities may be used to prevent interception of data being programmed onto an RFID tag. In addition or in the alternative, the fascia of the machine may include intrusion sensors adapted to sense radiation output by unauthorized RFID reading devices attached to the outside of the machine. The controller of the machine may be programmed responsive to detecting potential unauthorized RFID sensor signals to analyze the nature of the signals to determine if they correspond to those likely associated with an unauthorized reading device. In response to determining that such signals correspond to an unauthorized reading device, the controller may cause the machine to take actions in accordance with its programming. Such actions may include, for example, stopping operation of all or certain operations of the machine, such as cash dispensing operations. Actions may also include capturing a card from which data may have been intercepted. Actions may also include capturing image data from a camera. This may be accomplished, for example, in the manner shown in U.S. patent application Ser. No. 09/991,748 filed Nov. 23, 2001, the disclosure of which is incorporated herein by reference. Alternatively, such actions may include giving notice to a remote entity in a manner

IPR2025-01149
Apple EX1039 Page 15

such as is done in U.S. patent application Ser. No. 09/411,013 filed Oct. 1, 1999, the disclosure of which is incorporated herein by reference. The controller may also be operative to cause an emitter to output signals that are operative to jam, saturate or provide false data to an unauthorized RFID reading device. Of course, these actions are exemplary of actions that may be taken.

In some exemplary embodiments the data from an RFID tag may be used to authenticate other data on a user card or other item or feature used to operate an ATM. For example, data recoverable from memory on an RFID tag may be used to verify data recoverable from another source, such as a stripe or a chip on a card. For example, data read as part of RFID data may have a corresponding or other predetermined relationship to all or portions of magnetic stripe data, chip data, and/or customer input data. The presence of such a relationship can be determined through programmed operation of one or more controllers operating in the ATM. The determination that the relationship is present for the particular card or transaction may be used to provide greater assurance that the card is genuine and/or that data on the card has not been tampered with.

In some embodiments RFID tags can be embedded in cards or other items. In other embodiments an RFID tag may be attached to items. For example, a customer may be provided with a thin RFID tag that includes self adhesive material. The user may be provided by a card issuer, bank, or other entity with the RFID tag and given instructions to apply it to an associated magnetic stripe or other card. Data readable from the RFID tag can then be read by the ATM when the card is used, and such data compared to magnetic stripe and/or customer input data, or portions or combinations thereof for a determined relationship. The existence of the relationship serves to reduce the risk that the input card is genuine and is not a fraudulently produced duplicate card. The existence of the predetermined relationship can be required by the controller in accordance with its programming before ATM transactions such as dispensing cash can be conducted at the ATM.

In some embodiments the card issuer may provide replacement or additional self adhesive RFID tags to a card holder. The card holder may remove the existing RFID tag from the card and replace it with the new tag. The new tag may have different or additional data that can be utilized at the ATM controller to authenticate the card, the user, or other data, in another manner. ATMs may be programmed such that if the original tag is not replaced with the replacement tag, the card will no longer operate the ATM. Alternatively, the additional tag may need to be applied to the card while the first tag remains. The ATM controller may use data from both tags in the determination that the card should be accepted and the ATM operated to carry out one or more transaction functions.

Of course, these approaches are exemplary of approaches that may be used. Further, while the exemplary embodiment is used in conjunction with an ATM, it should be understood that similar principles may be used in conjunction with other credit card terminals, debit card terminals, vending devices and other devices that employ such cards for operation.

In still other embodiments an issuer of a card may provide a user with an RFID tag or other item that is not attached to or connected with the card. For example, the user may be provided with an item that includes an RFID tag that the user will always be expected to be carrying when the user conducts ATM transactions. This may include an item such as a card holding sleeve that the user can keep in a wallet, a tag that can be attached to a key ring, or a self adhesive label a user can attach to a key, watch, wallet, pen, jewelry or other item generally carried by the user. When the user conducts a transaction at the ATM, a reader in or operatively connected with the ATM reads RFID data from items in proximity to the ATM. If the proper RFID data is not detected, the ATM will not operate to perform at least some transactions. Thus even if a user's card data, card, and/or PIN has been taken by a criminal, the criminal may be prevented from accessing the user's account if the user does not have the personal item bearing the RFID data. Of course this approach is exemplary and in some embodiments other approaches may be used.

Further in some embodiments RFID tag data may include data usable for verifying the origin and/or authenticity of data or messages. For example, RFID data may include digital signatures and/or digital certificates. Such digital signatures and digital certificates could be used to authenticate data input via a card or through an input device, and/or could be used to authenticate a message originating from an ATM or other device and/or to verify the authenticity of data. Digital signatures and certificates can be used in ways similar to those described in the incorporated disclosures to verify the source of messages, to encrypt and decrypt data, and to configure an ATM. In some embodiments signature and/or certificate data may be wholly stored in an RFID memory, while in others only portions of such data, or data than can be used to resolve such signature or certificate data, can be stored in memory associated with an RFID source.

In other embodiments, data stored in connection with an RFID tag can be used to verify authenticity of a card and/or a user. For example, as previously discussed, a card issuer may provide a user with an RFID tag containing data. Such a tag may be a self adhesive tag to attach to the card or otherwise. Such a tag may include data that can be used by a controller in the machine to verify stripe or other card or user input data (PIN, biometric input, or other input, for example). Alternatively or in addition, the tag may have associated memory included therewith that includes data that can be used by the ATM to verify that the user is the authorized user of the card.

For example, the RFID tag may have stored thereon several items of information that only the authorized user is likely to readily know. These might include, for example, the last digit of the user's Social Security number, year of birth, first digit in residence address, first letter of street on which the user lives, first letter of mother's maiden name, first letter of mother's first name, first letter in father's first name, and other similar data. ATMs may be programmed to ask a customer a random (or in a predetermined order) one of these questions when a transaction session is initiated or at another time in a transaction session at the ATM. The input of the customer in response to the question is compared through operation of the controller in the ATM to the data read from the RFID tag. Only if the input data corresponds is the customer permitted to conduct a transaction or a selected transaction function.

In the exemplary approach, even if a customer's magnetic stripe data and PIN have been intercepted by a criminal, the criminal does not obtain sufficient information to use the card to conduct ATM transactions. In addition, even if the user's input in response to a question presented in response to one random question output by an ATM is intercepted, it has no value unless the criminal has been able to steal the card with the RFID tag or otherwise obtain the separate tag. Further, even if the criminal has the original RFID tag, because the exemplary ATM has a controller that is programmed to output the numerous questions randomly, the

customer's response that a criminal has been able to observe is not likely to be the correct response when the criminal presents the card at an ATM. Further, because the ATM can be programmed to capture the card in response to a set number of incorrect responses by a user, there is a significant chance the card will be captured and invalidated by an ATM before the criminal may use it in carrying out a transaction.

Similar approaches may be used with programmable RFID tags. In an exemplary approach, rather than having numerous possible answers to questions selected randomly stored in connection with the RFID tag, the RFID tag memory can be selectively programmed with data the customer may input through input devices on the ATM. For example, the ATM controller may be programmed to advise the customer that the time after the next time (or at some other later time) when the customer uses the card the customer will be asked to input particular data. This might be, for example, the first letter of the user's mother's first name. Data corresponding to the question and/or appropriate response would be input by the user to the ATM and be stored on the RFID tag through operation of the controller and RFID tag writer device. In an exemplary embodiment, the user can provide the question, answer, and/or a code for storage on the RFID tag. Then when the card is used on the corresponding subsequent occasion, the controller in the ATM would operate to present the question and verify the answer input by the user based on the RFID data, and enable at least one transaction or function with the ATM in response to receiving the correct input. Thus, even if a criminal stole the card, RFID tag (if separate from the card), PIN and the response given by the user, the criminal could not conduct a transaction at the ATM with the card, because the criminal would not know the correct response to the question the ATM would pose upon the next transaction (because it was input by the user during a prior transaction the criminal did not observe). Of course, this approach is merely exemplary.

It should be mentioned that some of these exemplary embodiments for verifying a user and/or a card or other item may be carried out locally at the ATM. This may avoid the need to modify the nature of transaction messages transmitted to and from the ATM in a financial network to carry out transactions. Of course other embodiments may use remote communication to facilitate secure operation. For example, a remote computer (connected to a data store) may provide one or more values or codes that are stored in RFID data. Such data (which may be in a card) may be looked for or used the next time the card is used, and its absence or variation identified to indicate a false or stolen card. Of course this approach is merely exemplary.

In alternative embodiments a user may be provided with a RFID tag that a user can install in or attach to an item such as a PDA with wireless communication capabilities or a cell phone. The PDA or cell phone associated RFID data may be read to initiate a transaction or a particular function at an ATM. For example, the RFID data may include data usually found on a card that corresponds to a user or user's account.

The ATM controller may be programmed to prompt the user after reading the RFID data to provide an input through the PDA or cell phone. For example, the ATM display could prompt the cell phone user to call a number associated with the ATM or a remote computer. The telephone connection could prompt the user to input the user's PIN through the cell phone. This could be used to reduce the risk of interception. Alternatively, the user could be instructed to change the user's usual PIN in a particular way for this transaction. For example, the user might be told via the phone connection to substitute a particular digit or symbol for the usual first PIN digit. The user would then input the modified PIN through the ATM, and the ATM would carry out the transaction. If a PDA is used, communication could be conducted wirelessly between the PDA and ATM such as through Bluetooth or other wireless communication. As can be appreciated, because the acceptable PIN could be varied with each transaction, a criminal observer of the input PIN would not have the user's actual PIN and the ability to conduct a transaction at an ATM.

Further, this exemplary approach could be combined with other approaches previously described to provide enhanced security. Of course these approaches are exemplary of many approaches that may be used.

An exemplary automated banking machine also has the ability to read non-card RFID devices. These RFID tags can be embedded in or associated with transaction items such as currency (e.g., bills and coins), checks, securities, account passbooks, certificates of deposit, tickets, coupons, gift certificates, etc. Documents such as present and next generation currency (e.g., plastic bills and plastic coins) can contain RFID tags. An RFID tag associated with a currency note can hold a plurality of information representative of the note, including but not limited to the note's value (e.g., $50), serial number, and issue date. The ATM may have an RFID tag reader that can read the note's RFID tag information. The ATM can also read the note's value, serial number, and issue date from one or more surfaces (faces) of the note. The ATM can perform a note validation process based on the read information. The note validation process can include checking whether the note face information read directly from the note matches the note face information read from the RFID tag. In alternative validation arrangements, the two sets of read note face information can be transmitted from the ATM to an ATM network host where the note validation process can be carried out.

Furthermore, the ATM or an ATM host or one or more remote computers or networks can transmit bank note validation information to a central processor arranged outside of the banking network in order to have the note validation process performed. The central processor can constitute one or more connected computers that comprise a main or central computer that maintains a data store containing data on all new (U.S.) currency bills. The data store includes note face information corresponding to particular RFID tag ID numbers and/or other data. The main computer may be a government (e.g., Treasury Department or Federal Reserve) computer.

In an example of a verification process, a bank note is received by an ATM in an attempted deposit transaction. The note has an RFID tag that only includes a tag ID number. The RFID tag can be non-programmable. Thus, the ID number is permanently assigned to that note. The ATM reads the note's face information. The ATM uses an RFID document tag reader to read the tag's ID number. The ATM gives the ID number (along with the information read from the face of the note) to the ATM host. The host passes the ID number and the note face information to the main computer. The main computer uses the ID number to obtain the note face information corresponding to that particular ID number from the data store. The main computer then compares the two sets of note face information to determine whether the note is valid. The main computer informs the ATM host on the determined validity of the particular note. The host can then instruct the ATM on whether to deposit, hold as suspicious, or return the note.

The use of RFID tags in currency permits tracking (or at least partial tracking) of currency. Tags can be used to track

IPR2025-01149
Apple EX1039 Page 17

the flow of money into and out of a banking network. For example, a banking network can use RFID tagged currency notes to monitor the activity of individual currency notes within the network. The monitoring can be used to enhance cash management. Cash can be reallocated to segments of the network in order to maintain a proper balance or to prevent a cash shortage situation. A network database can be used to store currency note inventory data. The database can be used to track the currency notes received into the banking network (e.g., deposits into ATMs, etc.) and the currency notes that have been removed from the banking network (e.g., ATM cash withdrawals, etc.). The inventory tracking may be carried out in real time. On a broader scale, the governmental main computer can be in communication with a plurality of banking network databases to access a real time inventory of cash over a wide segment of the banking industry. The main computer can be used by the Federal Reserve to reallocate cash throughout the different Federal Reserve regions.

The main computer can also be used to track currency for research. For example, the main computer can attempt to follow a currency note throughout its life cycle. The life of a currency note may include its creation at a mint, distribution by the Federal Reserve, passage through several banking systems, and multiple uses at several ATMs. The tracking can be used in note travel analysis. The tracking can also be used in detecting counterfeit currency, such as when a non existing serial number is detected or when two of the same serial numbers are detected in questionable situations. For example, a serial number read on the Eastern coast of the U.S. two hours after having been read on the Western coast would create a questionable situation.

RFID tags in currency can also be used in statistical analysis to calculate or create normal patterns of currency deposit. A pattern may include several factors, including a total deposit amount over a predetermined time period. A normal deposit pattern can be assigned to an individual ATM, a specific number of ATMs, and/or an entire network of ATMs. Patterns involving segments of an ATM network may also overlap. A normal deposit pattern can be created after performing a lengthy study (via RFID tags on currency) of deposits made to the ATMs assigned to the pattern's particular coverage area. For example, the pattern factor comprising the normal range of deposits per time period is calculated and assigned to that particular pattern. A pattern can be continually adjusted to compensate for different business activities (e.g., new housing) occurring within the pattern area.

The monitoring of deposit patterns (via RFID tags in currency) can be used to ascertain questionable deposit activity. The monitoring may be carried out in real time or near real time. In a pattern monitoring example, the pattern of currency entering an ATM network is compared to the normal deposit pattern for that network. A discovery is made that the current deposit pattern differs from the norm by an unacceptable range (e.g., 25%). The non normal pattern may be the result of an unusually large amount of currency having been deposited into several network ATMs within a relatively short period of time. Deposit patterns out of the norm are automatically flagged and may be investigated for illegal activity, such as money laundering. The previously discussed ability to use RFID tags to track deposited currency to a particular customer at a particular time can be used in the review of the flagged pattern to determine whether the deposit transactions were legitimate.

Other uses of currency with an RFID tag may also be used in exemplary embodiments. For example, an RFID tag with a programmable memory can be used to enhance the security of bank notes in an ATM. The ATM can operate an RFID writer to reprogram the RFID tag to change the status of currency between first and second identifier states (e.g., active and passive states). For example, a tag in a passive or non flagged state may represent that the currency note was legally dispensed and is valid for public usage. A tag in an active or flagged state represents that the currency note is (or should be) under the jurisdiction or ownership of a particular financial organization, such as a bank. An active note outside of the bank's currency system is an indication that the note was taken without permission (e.g., stolen) from the bank, such as via breaking into an ATM or during transport. Currency can be deactivated during its dispense from an ATM. Currency can be activated during its reception as a proper deposit. Of course this approach is merely exemplary.

The use of active and passive tags can prevent the laundering of a stolen note back into the banking system, such as via a deposit into an ATM. An ATM of the banking system can read the RFID tag of a note that is trying to be deposited, identify the note as active (suspicious or hot), and notify the proper authorities of the situation. Of course on a broader scale a banking system may be linked with other banking systems to share RFID tag information. Each bank may have a unique bank code that is represented in their active state of a tag. Each bank system can recognize not only their own currency but also that currency belonging to other banks via reading the bank code. A note without a tag may not be accepted for deposit. The serial number of a non-tagged note may be checked via a data store to determine if the note previously had a tag. A non-tagged note may be an indication that the tag was purposely removed or the note is counterfeit. Such tags may also be used to identify the particular individuals associated with transfers of particular bills.

In other programmable RFID tag arrangements a tag can be embedded in specialized currency. For example, programmable tags may be used in newly minted limited edition currency, large bills, or large securities. The tag can store an owner-chosen or other type data such as an encrypted PIN. The PIN may serve as an additional security feature to verify that the current possessor is the actual legal owner. Only specific entities (e.g., banks, security dealers) may have access to the authorized readers that are necessary to decrypt and read a PIN. A provided or entered PIN can be compared with the PIN stored in the RFID tag of the bill or security. Upon transfer of a security the PIN can be changed by the new owner.

The capability of an ATM to use an RFID tag to recognize an individual item and associate the particular item to a particular customer/account can also be applied to financial checks. A check may include an RFID tag. The check's RFID tag can be programmable. A check's RFID tag can initially contain information representative of the maker's name, account number, and bank name. As previously discussed, the ATM can have an RFID tag reader/writer. The ATM can add information to the tag, modify the tag, or reprogram the tag. For example, additional information that may be added to the tag by the ATM may include the check amount, date, payor, payee, transmitting bank, routing number, and/or bank account or other data or numbers. The ATM prepares the tag memory so that all the necessary information is available in the RFID tag to allow the Federal Reserve to read the tag and process (clear) the check.

In an exemplary embodiment the component modules/devices (e.g., input and output devices) inside of an automated banking machine use contactless (e.g., wireless) pro-

IPR2025-01149
Apple EX1039 Page 18

cesses to communicate with each other and/or to the machine's internal computer(s). The internal ATM controller(s) can serve as a local host computer to each of the components in the machine. It should also be understood that the local host computer can also constitute a machine component. As previously discussed, automated banking machine components may include (but are not limited to) transaction function devices such as any of a card reader, keypad, function keys, display, receipt printer, journal printer, account statement printer, currency dispenser, and currency acceptor. Wireless communication can be used to make the individual components independent of any hard-wired signal communication relying on wiring or distribution hubs. That is, the components can have wireless communication that is not dependent on any fixed hard wiring between components. Interface hub wiring (e.g., USB hubs) for multiple device interfaces can be reduced or eliminated.

A wireless communication arrangement frees up additional room inside of an ATM housing and makes component placement more flexible. Thus, additional functionality and/or more devices/components can be added to the ATM. The number of module/device interfaces and locations can be increased in the ATM. The number of devices is not limited by the number of individual hard-wired signal/communication wires, distribution hubs, or their physical locations inside the ATM. Some components that do not have to be located adjacent a fascia opening may be randomly positioned in the machine, due to their exact position being irrelevant. Troubleshooting, component/machine downtime, and replacement of faulty hard wiring associated with communication wiring between the ATM's internal computer and a component can also be reduced or eliminated. Power supply to devices can also be provided in some embodiments by providing RF energy within the housing from one or more emitters. Multiple transaction function devices may receive power from the RF emitter(s) as necessary for operation and/or communication.

A wireless communication arrangement may also be used to add an additional layer of security to an ATM by reducing the opportunity to tamper with an ATM and/or its components. Elimination of component hard-wiring removes the ability of a person to physically alter wiring to provide unauthorized access to the ATM banking network and/or to control an ATM component. With the absence of wiring, then any capacity to bypass original hard wiring with false wiring between a local host computer and the components for the purpose of overriding original programming has been eradicated.

Communication among the components and the host computer can utilize encryption codes as an additional security layer. Likewise, communication involving an RFID device can be encrypted. The encryption codes can be utilized as an additional security layer in sensing, indicating, and/or reporting when suspected tampering is occurring.

A component's RFID device can be activated by another component (or an RFID device of that component) during an attempt to communicate. When activated the RFID device can automatically power up its component in order to receive data and/or transmit requested data. A component can be arranged such that it is only powered up (i.e., "on") when its RFID device is in an active state. An RFID device can also be used to automatically power down its component upon an instruction (e.g., deactivation signal) or during absence of activity. Power consumption of a component can be reduced by installing a "sleep" mode in the component.

The ATM housing can be shielded with RF blocking materials to prevent interference, interception, or outside manipulation of the communications among the components and the host computer. A shielding structure may include conductive elastomer.

FIG. **11** shows a rear view of components and a host computer **94** arranged in an interior portion of an ATM **92**. The components and host computer are devoid of wired communication with each other, but can communicate with each other wirelessly. Components such as a card reader **95**, display **96**, currency dispenser **97**, and currency acceptor **98** are shown.

As previously discussed, the use of RF can eliminate mechanical contact between cards and card readers. Of course the use of radio frequency is one example of non-contacting remote communication. It should be understood that other types of non-contacting information communication may be used in other exemplary embodiments instead of (or in additional to) radio frequency or radio waves.

Thus, the new and improved automated banking machine features achieve at least one of the above stated objectives, eliminate difficulties encountered in the use of prior devices and systems, solve problems, and attain the desirable results described herein.

In the foregoing description certain terms have been used for brevity, clarity and understanding, however no unnecessary limitations are to be implied therefrom because such terms are used for descriptive purposes and are intended to be broadly construed. Moreover, the descriptions and illustrations herein are by way of examples and the invention is not limited to the details shown and described.

In the following claims any feature described as a means for performing a function shall be construed as encompassing any means known to those skilled in the art capable of performing the recited function, and shall not be limited to the structures shown herein or mere equivalents thereof.

Having described the features, discoveries and principles of the invention, the manner in which it is constructed and operated, and the advantages and useful results attained; the new and useful structures, devices, elements, arrangements, parts, combinations, systems, equipment, operations, methods, processes and relationships are set forth in the appended claims.

I claim:

**1**. Apparatus including:

an automated banking machine,

wherein the machine includes a currency dispenser,

wherein the currency dispenser is operative to dispense currency notes from the machine,

wherein the machine includes a user card receiving slot,

wherein the slot is operative to receive at least a portion of a user card inserted therein,

wherein the machine includes therein a magnetic stripe reader positioned adjacent the slot,

wherein the magnetic stripe reader is operative to read data from a card magnetic stripe inserted in the slot,

wherein the machine includes therein an RFID tag reader positioned adjacent to the magnetic stripe reader and the slot,

wherein the tag reader is operative to read data from a card RFID tag inserted in the slot,

wherein the machine is operative to use data read from a user card in carrying out a transaction including operation of the currency dispenser.

**2**. The apparatus according to claim **1** wherein the machine includes at least one controller and at least one user input device, wherein the at least one user input device is

IPR2025-01149
Apple EX1039 Page 19

operative to receive at least one user input corresponding to a card, and wherein the controller is operative to enable the machine to carry out at least one transaction function responsive to at least a portion of at least one of stripe data and tag data corresponding to the at least one user input.

**3**. The apparatus according to claim **2** wherein the at least one user input device comprises at least one key, and wherein the at least one user input comprises actuating at least one key of the at least one user input device.

**4**. Apparatus comprising:

an automated banking machine,

wherein the machine includes a currency dispenser,

wherein the currency dispenser is operative to dispense currency notes from the machine,

wherein the machine includes a magnetic stripe reader,

wherein the magnetic stripe reader is operative to read data from at least one magnetic stripe of a user card,

wherein the machine includes an RFID tag reader,

wherein the tag reader is operative to read data from at least one RFID tag of a user card,

wherein the machine includes at least one controller including at least one processor,

wherein the at least one controller is in operative communication with both the magnetic stripe reader and the RFID tag reader,

wherein the at least one controller is operative to cause the magnetic stripe reader to read stripe data from at least one stripe of a user card and the RFID tag reader to read tag data from at least one RFID tag of the user card,

wherein the at least one controller is operative to determine if at least a portion of the stripe data and at least a portion of the tag data have a predetermined relationship.

**5**. The apparatus according to claim **4** wherein the automated banking machine includes a user card insertion slot, wherein the magnetic stripe reader is operative to read data from a magnetic stripe of a user card inserted into the slot, and wherein the RFID tag reader is operative to read data from an RFID tag of a user card inserted into the slot.

**6**. The apparatus according to claim **4** wherein the machine includes at least one user input device in operative connection with the at least one controller, wherein the at least one user input device is operative to receive at least one user input corresponding to the card, and wherein the controller is operative to enable the machine to carry out at least one transaction function responsive to a positive determination.

**7**. The apparatus according to claim **4** wherein, responsive to determining the predetermined relationship, the at least one controller is operative to enable the machine to carry out at least one transaction function.

**8**. The apparatus according to claim **7** wherein the at least one transaction function includes dispensing currency notes from the machine through operation of the currency dispenser.

**9**. The apparatus according to claim **8** wherein the machine includes at least one user input device in operative connection with the at least one controller, and wherein the at least one user input device is operative to receive at least one user input corresponding to the card, and wherein the controller is operative to enable dispensing currency notes responsive to at least a portion of at least one of the stripe data and tag data corresponding to the at least one user input.

**10**. The apparatus according to claim **9** wherein the at least one user input device comprises at least one key, and the at least one user input comprises actuating at least one key.

**11**. The apparatus according to claim **10** wherein the at least one user input device comprises a keypad having a plurality of keys, and wherein the at least one user input comprises pressing at least one key of the keypad.

**12**. The apparatus according to claim **11** wherein the at least one user input comprises a PIN.

**13**. The apparatus according to claim **12** wherein the PIN corresponds to the stripe data.

**14**. The apparatus according to claim **9** wherein the at least one input device comprises a biometric input device.

**15**. The apparatus according to claim **9** wherein the machine comprises at least one output device and wherein the at least one controller is operative to cause the machine to output at least one question through the at least one output device, and wherein the controller is operative to enable dispensing currency notes responsive to at least one answer input provided through the at least one input device responsive to the at least one question.

**16**. The apparatus according to claim **15** wherein the controller is operative to determine if the answer input has a predetermined relationship to at least a portion of the tag data.

**17**. The apparatus according to claim **16** wherein the data includes data corresponding to a correct answer to the at least one question, and wherein the controller is operative to determine if the answer input corresponds to a correct answer.

**18**. The apparatus according to claim **16** wherein the at least one controller is operative to output a plurality of questions, and wherein the tag data includes data corresponding to correct answers to a plurality of questions.

**19**. The apparatus according to claim **18** wherein the at least one controller is operative to present the questions randomly.

**20**. The apparatus according to claim **16** wherein the at least one controller is operative to output the at least one question responsive to at least a portion of the tag data.

**21**. The apparatus according to claim **20** wherein the machine includes at least one RFID tag writer, and wherein the at least one controller is operative to cause the machine to output at least one additional question, and to receive at least one additional answer input through the at least one input device, and wherein the controller is operative to cause the tag writer to store data corresponding to the at least one additional answer in the tag data.

**22**. The apparatus according to claim **21** wherein the at least one controller is operative to cause data corresponding to the at least one additional question to be stored in the tag data.

**23**. The apparatus according to claim **22** wherein the at least one question is output responsive to at least a portion of data stored in the tag data during a prior banking machine transaction session.

**24**. The apparatus according to claim **23** wherein the at least one controller is operative to output the at least one question responsive to at least a portion of the data stored in the tag data during other than an immediately preceding transaction session.

**25**. The apparatus according to claim **24** when the tag data includes at least one of a digital signature and a digital certificate, and wherein the controller is operative to deter-

mine authenticity of at least one of a message and data through use of the at least one of the digital certificate and digital signature.

**26**. The apparatus according to claim **25** wherein the tag reader is operative to read a plurality of RFID tags on the card, and wherein the at least one controller is operative to enable dispensing currency responsive to the tag data read from the plurality of tags.

**27**. The apparatus according to claim **26** wherein the machine further includes an RFID document reader, and where the at least one controller is operative to cause the document reader to read document data on RFID tags included on documents that are at least one of placed in or dispensed from the machine.

**28**. The apparatus according to claim **27** wherein the document reader is operative to read document data on checks placed in the machine.

**29**. The apparatus according to claim **27** wherein the document reader is operative to read document data on currency placed in the machine.

**30**. The apparatus according to claim **27** wherein the document reader is operative to read document data on currency dispensed from the machine.

**31**. The apparatus according to claim **27** wherein the machine further includes an RFID document writer, and wherein the at least one controller is operative to cause the document writer to change document data on RFID tags included on documents that are at least one of placed in and dispensed from the machine.

**32**. The apparatus according to claim **31** wherein the document writer is operative to change document data on checks placed in the machine.

**33**. The apparatus according to claim **31** wherein the document writer is operative to change document data on currency placed in the machine.

**34**. The apparatus according to claim **31** wherein the document writer is operative to change document data on currency dispensed from the machine.

**35**. The apparatus according to claim **31** and wherein the controller is operative to communicate wirelessly through radio frequency messages in the housing with at least one of the tag reader, magnetic stripe reader, document reader, and document writer.

**36**. The apparatus according to claim **35** and further including a user card having at least one of an RFID tag and a magnetic stripe.

**37**. The apparatus according to claim **27** wherein the machine comprises a housing wherein at least one of the tag reader, document reader, and document writer are positioned within the housing, and wherein the housing comprises radio frequency signal blocking material.

**38**. The apparatus according to claim **37** and further comprising at least one intrusion sensor adapted to sense unauthorized RFID sensors adjacent the housing, wherein the at least one intrusion sensor is in operative connection with the at least one controller, and wherein the at least one controller is operative to cause the machine to take at least one action responsive to a sensing by the at least one intrusion sensor.

**39**. The apparatus according to claim **21** wherein the at least one controller is operative to cause the tag writer to overwrite tag data.

**40**. The apparatus according to claim **4** and further comprising a card, and wherein the at least one RFID tag is releasably attached to the card.

**41**. Apparatus including:

an automated banking machine,

wherein the machine includes a currency dispenser,

wherein the currency dispenser is operative to dispense currency notes from the machine,

wherein the machine includes a magnetic stripe reader,

wherein the magnetic stripe reader is operative to read data from at least one magnetic stripe of a user card,

wherein the machine includes an RFID tag reader,

wherein the tag reader is operative to read data from at least one RFID tag of a user card,

wherein the machine is operative to read data from a user card using at least one of the magnetic stripe reader and the RFID tag reader,

wherein the machine includes at least one controller including at least one processor,

wherein the at least one controller is operative to cause the magnetic stripe reader and the RFID tag reader to respectively read stripe data from the at least one magnetic stripe and tag data from the at least one RFID tag.

**42**. The apparatus according to claim **41** wherein the machine includes a user card insertion slot, wherein the magnetic stripe reader is operative to read data from a magnetic stripe of a user card inserted into the slot, and wherein the RFID tag reader is operative to read data from an RFID tag of a user card inserted into the slot.

**43**. The apparatus according to claim **41** wherein the machine includes at least one user input device in operative connection with the at least one controller, wherein the at least one user input device is operative to receive at least one user input corresponding to the card, and wherein the controller is operative to enable dispensing currency responsive to at least a portion of at least one of the stripe data and tag data corresponding to the at least one user input.

**44**. The apparatus according to claim **43** wherein the at least one user input device comprises at least one key, and the at least one user input comprises actuating at least one key.

**45**. The apparatus according to claim **41** wherein the machine comprises at least one output device, and wherein the at least one controller is operative to cause the machine to output at least one question through the at least one output device, and wherein the controller is operative to enable dispensing currency responsive to at least one answer input provided through the at least one input device responsive to the at least one question.

**46**. The apparatus according to claim **45** wherein the at least one controller is operative to determine if the answer input has a predetermined relationship to at least a portion of the tag data.

**47**. The apparatus according to claim **46** wherein the at least one controller is operative to output a plurality of questions, and wherein the tag data includes data corresponding to correct answers to a plurality of questions.

**48**. The apparatus according to claim **45** wherein the at least one controller is operative to present the questions randomly.

**49**. The apparatus according to claim **45** wherein the at least one controller is operative to output the at least one question responsive to at least a portion of the tag data.

**50**. The apparatus according to claim **49** wherein the machine includes at least one RFID tag writer, and wherein the at least one controller is operative to cause the machine to output at least one additional question and to cause the machine to receive at least one additional answer input

through the at least one input device, and wherein the controller is operative to cause the tag writer to store data corresponding to the at least one additional answer in the tag data.

**51**. The apparatus according to claim **50** wherein the at least one controller is operative to cause data corresponding to the at least one additional question to be stored in the tag data.

**52**. The apparatus according to claim **51** wherein the at least one question is output responsive to at least a portion of data stored in the tag data during a prior banking machine transaction session.

**53**. The apparatus according to claim **41** when the tag data includes at least one of a digital signature and a digital certificate, and wherein the controller is operative to determine authenticity of at least one of a message and data through use of the at least one of the digital certificate and digital signature.

**54**. The apparatus according to claim **41** wherein the controller is operative to cause the tag reader to read tag data from a plurality of RFID tags on a user card, and wherein the controller is operative to enable the operation of the currency dispenser to dispense currency notes responsive to the tag data read from the plurality of tags.

**55**. The apparatus according to claim **41** wherein the machine further includes an RFID document reader, and where the at least one controller is operative to cause the document reader to read document data on RFID tags included on documents that are at least one of placed in and dispensed from the machine.

**56**. The apparatus according to claim **41** wherein the machine further includes an RFID document writer, and wherein the at least one controller is operative to cause the document writer to change document data on RFID tags included on documents that are at least one of placed in and dispensed from the machine.

**57**. The apparatus according to claim **41** and further comprising at least one intrusion sensor adapted to sense unauthorized RFID sensors adjacent the housing, wherein the at least one intrusion sensor is in operative connection with the at least one controller, and wherein the at least one controller is operative to cause the machine to take at least one action responsive to a sensing by the at least one intrusion sensor.

* * * * *